ПАМЯТКА
«О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ»

Сохранность денежных средств и банковской карты во многом зависит от самого держателя, его знаний пользования картой, соблюдении мер безопасности, а также осведомлённости о схемах мошенничества с банковскими картами, используемых преступниками.

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность банковской карты, её реквизитов, ПИН и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Общие рекомендации Держателям Карт

Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам Банка, кассирам и лицам, помогающим Вам в использовании банковской карты.

1. ПИН необходимо запомнить или, в случае если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.
2. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.
3. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.
4. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
5. Телефон Банка-эмитента (т.е. Банка, который выдал банковскую карту), указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны Банк-эмитента и номер банковской карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН.
6. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета, целесообразно установить суточный лимит на сумму операций по банковской карте и. одновременно, подключить электронную услугу оповещения о проведенных операциях - **услугу «SMS-банкинг»**.
8. При получении просьбы, в том числе со стороны сотрудника Банка, сообщить персональные данные или информацию о банковской карте (в том числе ПИН), не сообщайте их. Перезвоните в Банк (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.
9. Не рекомендуется отвечать на электронные письма, в которых от имени Банка предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт Банк), т.к. они могут вести на сайты-двойники.
10. В целях информационного взаимодействия с Банком-эмитентом рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке-эмитенте.

11.Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц.

В случае если, имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также, если банковская карта была утрачена, необходимо немедленно обратиться в Банк-эмитент и следовать указаниям сотрудника данного Банка. До момента обращения в Банк-эмитент Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Согласно условиям договора с Банком-эмитентом, денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом Банка-эмитента, не возмещаются.

12.Также необходимо регулярно проверять выписки с вашего банковского счета, а также контролировать остаток по карте. В случае малейшего несоответствия необходимо незамедлительно обратиться в Банк за разъяснениями.

Рекомендации при совершении операций с банковской картой в банкомате

Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

1. Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.

2. Перед использованием банкомата осмотритесь вокруг, не следует проводить операцию по пластиковой карте в присутствии подозрительных людей, или если банкомат выглядит небезопасно или слишком изолированно.

3. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.

4. Банкомат не должен выглядеть подозрительно; следует проверить, не прикреплены ли к банкомату какие-либо дополнительные устройства; на экране банкомата не должно быть никаких дополнительных инструкций, а также вызывающих сомнение пустых экранов.

6.Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.

7.Набирайте ПИН таким образом, что бы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН прикрывайте клавиатуру рукой.

8. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку «Отмена», и дождаться возврата банковской карты.

9. После получения наличных денежных средств в банкомате, следует пересчитать банкноты полистно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем доложить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

10.Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.

11.Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.

12. Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в Банк по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в Банк-эмитент (Банк, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника Банк.

Рекомендации при использовании банковской карты для безналичной оплаты товаров и услуг

Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
1. Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.

2. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем, как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.
3. В случае если при попытке оплаты банковской картой имела место «не успешная» операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

Рекомендации при совершении операций с банковской картой через сеть Интернет

Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
1. Не сообщайте персональные данные или информацию о банковской (ом) карте (счете) через сеть Интернет, например, ПИН, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.
2. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.
3. Следует пользоваться Интернет-сайтами только известных и проверенных организаций торговли и услуг.
4. Обязательно убедитесь в правильности адресов Интернет-сайтов, к которым подключаетесь, и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.
5. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской (ом) карте (счете).
В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).
6. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

Известные схемы мошенничества по картам

Наиболее распространенными схемами мошенничества с банковскими картами по данным **APACS** (Association for Payment Clearing Services - Ассоциация систем клиринговых платежей - Великобритания), являются следующие:

Оглашение сведений о ПИН-коде самим держателем карты. Имеется ввиду, к примеру, запись ПИН-кода на карте или каком-либо носителе (лист бумаги, записная книжка, мобильный телефон), хранимом вместе с картой. Соответственно, если карта утеряна или украдена (вместе с сумкой, бумажником), у мошенника оказывается и карта и персональный код.

- **Дружественное мошенничество**. Использование в своих целях карты с предварительной осведомленностью о ПИН-коде членами семьи, близкими друзьями, коллегами по работе. То есть людьми, имеющими доступ к месту хранения карты.

- **Подглядывание из-за плеча**. Мошенник вполне может узнать ПИН-код держателя банковской карты, подглядывая из-за его плеча, пока тот вводит код в банкомате. Затем злоумышленник осуществляет кражу карты и использует ее в своих целях.

- **"Ливанская петля"**. Как вариант подглядывания из-за плеча. Пока владелец карточки погружает ее в банкомат, она застревает. В это время подходит "советчик", который рекомендует срочно идти и звонить в сервисную службу, к примеру. Владелец карты уходит, а тем временем "советчик", видевший как он набирал ПИН-код, вытаскивает карту и снимает деньги.

- **Фальшивые банкоматы**. Мошенники разрабатывают и производят фальшивые банкоматы, либо переделывают старые, которые выглядят как настоящие. Размещаются банкоматы в наиболее оживленных местах. После введения карты и ПИН-кода обычно на дисплее фальшивого банкомата появляется надпись, что денег в банкомате нет или, что банкомат не исправен. К тому времени мошенники уже скопировали с магнитной полосы карты информацию о счете данного лица и его персональный идентификационный номер.

- **Копирование магнитной полосы (skimming)**. Данный вид мошенничества предусматривает использование особых видов устройств, считывающих информацию с магнитных полос карт. Обычно это специально изготовленные клавиатуры, которыми накрывают существующие. Законный держатель банковской карты проводит операцию с вводом персонального идентификационного номера (ПИН), в это время, дополнительно установленное устройство считывает и записывает информацию на магнитной полосе. Т.е. у злоумышленников появляется данные необходимые для дальнейшего изготовления поддельной карты и ее использования в своих целях.

- **Ложный ПИН-ПАД**. Держателю карты может быть предложено ввести ПИН-код не в настоящий ПИН-ПАД (устройство для ввода ПИН-кода), а в его имитацию, которая запомнит введенный код. Такие ложные устройства иногда устанавливают рядом со считывающими датчиками, предназначенными для прохода в помещение с банкоматом с использованием в качестве идентификатора (электронного ключа) банковской карты.

- **Ограбление держателей банковских карт**. Самый незамысловатый способ. Клиент снял наличность - мошенник ограбил.

- **Фишинг (от англ. Phishing)**. В вольном переводе "закидывание удочки". Термин появился для обозначения новых схем, в результате которых путем обмана становятся доступны реквизиты банковской карты и ПИН-код. Чаще всего используется в виде рассылки через Интернет писем от имени банка или платежной системы с просьбой подтвердить

указанную конфиденциальную информацию на сайте организации.

- **Вишинг (англ. vishing)** - новый вид мошенничества - голосовой фишинг, использующий технологию, позволяющую автоматически собирать информацию, такую как номера карт и счётов. Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию:

  - автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции - перезвонить по определенному номеру немедленно. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, часто представляется вымышленным именем от лица финансовой организации;

  - когда по этому номеру перезванивают, на другом конце провода отвечает типично компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона;

  - как только номер введен, вишер становится обладателем всей необходимой информации (номер телефона, полное имя, адрес), чтобы, к примеру, обложить карту штрафом;

  - затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как PIN-код, срок действия карты, дата рождения, номер банковского счета и т.п.

- **Неэлектронный фишинг**. Данный вид связан с осуществлением покупок в торговых организациях посредством обязательного ввода ПИН-кода. В схемах неэлектронного фишинга создаются реальные торгово-сервисные предприятия/офисы банков, либо используются уже существующие. Держатели платежных карт совершают покупки товаров, получают услуги либо снимают денежные средства в кассе банка. Операции производятся с использованием банковских микропроцессорных карт и сопровождаются введением клиентом своего ПИН-кода. Сотрудники мошеннических предприятий негласно копируют информацию с магнитной полосы карты и производят запись персонального идентификационного номера. Далее мошенники изготавливают поддельную банковскую карту, и в банкоматах производится снятие денежных средств со счета клиента.

- **Вирус, поражающий банкоматы**. Новейшим изысканием мошенников стал вирус, который отслеживает производимые операции и ворует информацию с пластиковых карт, передавая ее мошенникам. Написать вредоносную программу для банкомата очень сложно - мошенники используют очень специфические операционные системы и связываются с банками по серьезно защищенным сетям.

Существует множество способов обмана …..!
Если вы стали жертвой преступления Вам необходимо в срочном порядке обратиться в Дежурную часть ОМВД РФ по городу Нефтеюганску по адресу: 8 «А» мкр., 56 дом. Телефон: 02 (с сот. 112) 295611; 295610. Телефон доверия: 247511

БУДЬТЕ БДИТЕЛЬНЫ!!!